CDSL/OPS/DP/POLCY/2021/207 **May 04, 2021**

CYBER SECURITY ADVISORY – STANDARD OPERATING PROCEDURE FOR HANDLING CYBER SECURITY INCIDENTS OF INTERMEDIARIES

As per SEBI Directives, Member Brokers / Participants / Intermediaries shall maintain Standard Operating Procedures (SOP) with respect to handling of Cyber Security Incidents.

Basis the said SEBI directive, Member Brokers / Participants / Intermediaries are hereby advised to formulate and adhere with the SOP for handling and reporting of Cyber Security Incidents.

The following aspects shall form part of the SOP which needs to be complied with by Member Brokers / Participants / Intermediaries:

- Members shall have documented Cyber Security incident handling process document i.e., Standard Operating Procedure (SOP) in place.
- Members shall examine the incidents and classify the incidents into High / Medium / Low as per their cyber security incident handling document.
- The cyber security incident handling document shall define Actions / Response Mechanisms for the incident based on severity.
- Members shall report the incident to Indian Computer Emergency Response Team (CERT-In).
- Members shall provide the reference details of the reported incident to the Depository and SEBI. Members shall also provide details regarding whether CERT-In team is in touch with the members for any assistance on reported incident. If the incident is not reported to CERT-In, members shall submit the reasons for the same to the Depository and SEBI.
- Members shall communicate with CERT-In / MHA / Cybercrime police for further assistance on the reported incident.
- Members shall submit details on whether the incident has been registered as a complaint with law enforcement agencies such as Police or cyber security cell. If yes, details need to be provided to Depository and SEBI. If not, reason for not registering complaint should also be provided to Depository and SEBI.
- The details of reported incidents and submission to various agencies by the member shall also be submitted to Division Chiefs (in charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI.
- The Designated Officer of the Member (appointed in terms of para 6 of the SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events within

24 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter.

All DPs are advised to ensure compliance with the above regulatory requirements.

References:

- SEBI Circular "SEBI/HO/MIRSD/CIR/PB/2018/147"; Dated December 03, 2018 on "Cyber Security and Cyber Resilience Framework for Stock Brokers / Depository Participants".
- CDSL Communique: CDSL/OPS/DP/POLCY/2019/375 dated 06th July 2019.
- CDSL Communique: CDSL/OPS/DP/POLCY/2019/535 dated 23rd October 2019.

Queries regarding this communiqué may be addressed to CDSL – Helpdesk: on telephone numbers (022) 2305-8624, 2305-8639, 2305-8642, 2305-8663, 2305-8640, 2300-2041 or 2300-2033. Emails may be sent to: dpinfosec@cdslindia.com or helpdesk@cdslindia.com.

sd/-

Rajesh Nadkarni
Chief Information Security Officer